REMARKS

The above amendment and these remarks are responsive to the Office Action of Examiner Daniel J. Ryman, dated 29 Mar 2005.

Claims 1, 3-14, and 16-22 are in the case, none as yet allowed.

Drawings

The Examiner requires that Figure 1 be labeled PRIOR ART. Applicants submit herewith a REPLACEMENT SHEET bearing the required label, and requests that it be accepted and entered into the case.

The Examiner objects to the drawings for failure to refer in the specification to the following reference characters: 158, 162, and 170.

With respect to reference character 158, this is described at page 16, line 4, as follows:

Referring to Figure 4, VPN NAT source-in executes to translate IDci for responder-mode conversations as follows: in step <-2>, for remotely initiated conversations, at start, since NAT is requested, implicit MAP rule 158 <MAP ihs TO rhs> is created, copying responder mode NAT flag IDci 152 to rhs 154. [Specification, page 16, lines 1-6, emphasis added].

With respect to reference characters 162 and 170, while these values are present, they do not figure in the present invention, and as is apparent from an examination of Figure 4, the values are not changed as a result of executing the method of the invention. That is, this type of VPN NAT does not change the inbound destination IP address nor does it change the outbound source IP address, and Figure 4 indicates such by there being no lines in or out from them. Thus, without the addition of new matter, Applicants have amended the specification at page 16 to state as follows:

(Note that the inbound destination IP address 170 and the outbound source IP address 162 are not changed.).

Specification

The Examiner, in objecting to the specification, has identified a several typographical errors, all of which have been corrected by Applicants in this response.

Further, Applicants have updated the references to related applications as requested by the Examiner.

35 U.S.C. 112

Claim 2 has been rejected under 35 U.S.C. 112, second paragraph.

Applicants have canceled claim 2.

35 U.S.C. 102

Claims 1, 3-6, and 10 have been rejected under 35 U.S.C. 102(b) over Srisuresh (P. Srisuresh, "RFC 2709 - Secuirty Model with Tunnel-mode IPsec for NAT Domains". Network Working Group, RFC 2709, October 1999. 1-9).

Regarding claims 1 and 10, Srisuresh does not disclose certain claimed aspects of the current invention.

First, Srisuresh does not use, mention, or disclose "an outer connection and an inner connection", by which it is clear in the current invention is meant two IPsec connections, one nested inside the other (see Fig. 2 and explanatory text at Page 10, lines 17-20). Srisuresh does mention tunnel mode IPsec, which is not the same as two nested IPsec connections (please refer to summary information below on IPsec). In the current invention the two IPsec connections may independently be IPsec in transport mode or tunnel mode, and this is completely independent of the fact that they have a nested relationship. Hence, in the current invention all possible combinations are supported; transport mode inside tunnel mode, transport mode inside transport mode, tunnel mode inside tunnel mode and tunnel mode inside transport mode. Srisuresh does mention an IP-IP tunnel (section 2.2), but this is not an IPsec connection. Hence any traffic inside this IP-IP tunnel is not inside an 'outer connection'. Srisuresh does mention that the IP-IP tunnel may contain IPsec traffic (an IPsec connection), but this is not what is claimed in the current invention, in claim 1, lines 1-5.

Claims 1 and 10 have been amended to make clear that the outer and inner connections are IPsec connections.

Second, Sirsuresh does not deal with two IPsec connections with coincident endpoints, as claimed. He does have his IPC-NAT as the NAT node at apparently an endpoint of his IP-IP tunnel (2.2). But, of course, this is not the same as two IPsec connections with coincident endpoints, nor is it the same as two IPsec connections one nested inside the other, with coincident endpoints at 'a first node'. Sirsuresh's IPC-NAT and the current invention's VPN NAT (source-in) are both coincident with an endpoint of an IPsec tunnel, but this is not what the current invention claims. Hence, on this point, Sirsuresh does not anticipate the current invention.

Third, to appreciate the next claimed difference between Sirsuresh and the current invention, note that Sirsuresh repeatedly focuses the RFC and descriptions on 'tunnel mode IPsec' ("...capable of offering tunnel-mode IPsec security..." p1 abstract; "... can benefit from IPsec tunnel-mode security, when the NAT device acts as the IPsec tunnel end point." p2 2nd paragraph; "For purposes of this document, we will assume IPsec security to means tunnel mode

IPsec security..." p3 1st paragraph of section 3; <and others>). The current invention, throughout the text simply refers to IPsec connections, making no distinction to whether or not any of the IPsec connections are tunnel mode or transport mode. This is because the current invention applies to both modes of IPsec connections. And while Sirsuresh does not seem to explicitly rule out transport mode IPsec, he does so in effect. Hence, on this point Sirsuresh does not anticipate the current invention.

Fourth, concerning the last clause of claim 1; some elements of Sirsuresh and the current invention are similar, but even so, Applicants argue, Sirsuresh does not anticipate the claim. Similar elements are that NAT (some kind) is performed on the outbound packet, and the NAT is done on the same node as the endpoint of an IPsec tunnel. However, in Applicants' claims, since two IPsec connections are being used, one nested inside the other, the source-in NAT associated with the inner IPsec connection must be done prior to its encapsulation in both IPsec connections; this is not anticipated by Sirsuresh (which does not use nested IPsec connections).

Regarding claim 3 -- claim 3 deals with particulars of

setting up the two, nested IPsec connections as shown in Fig 2 of the current invention, such that they work. That is, in such a manner that source-in VPN NAT can be configured for the outer T1 52 IPsec connection, and this will automatically and correctly be applied to the later established inner T2 54 IPsec connection. Since Sirsuresh does not deal with nested IPsec connections, it clearly does not anticipate claim 3 in general. And less so in any of the following particulars.

First, more specifically, Sirsuresh does not configure an outer IPsec connection as the Examiner states (Office Action, paragraph 11); how could it since it does not deal with nested IPsec connections.

Second, Sirsuresh does not teach "communicating from a client to a gateway on said outer connection a request to configure a secure inner connection". Sirsuresh does not do this at pages 5-6, section 4 or Fig 5, to which the Examiner refers. Sirsuresh does not have an outer IPsec connection.

Third, Sirsuresh states, again (Page 5, 1st paragraph of section 4), "In other words, we will focus on the operation of IKE in conjunction with tunnel mode IPsec...".

The current invention works for all IPsec modes, and for both AH and ESP protocols, and all combinations thereof.

Fourth, with respect to the 3rd clause of claim 3, Sirsuresh does teach this; "IKE will communicate the negotiated security parameters directly to the IPC-NAT gateway engine as described in the following diagram.", referring to Sirsuresh Fig. 5. This is an aspect of similarity between Sirsuresh and current invention; both involve communicating something from IKE to something related to NAT. Sirsuresh uses 'policies', and the current invention uses IPsec Security Associations. However, since Sirsuresh does not deal with nested IPsec connections, he does not anticipate "initializing said gateway to receive a future nested communication". This initialization contains the specifics for source-in NAT, the use of the address pool, generating the implicit MAP rule and loading the VPN NAT implicit MAP rule. None of these technical specifics is anticipated by Sirsuresh.

Fifth, Sirsuresh does not teach 'starting said inner connection'.

Sixth, Sirsuresh does not teach the last clause of

claim 3; "responsive to starting said inner connection, propagating a network address translation rule from said outer connection to said inner connection". This step relates functioning and automatic setup of nested IPsec connections with VPN NAT, because (as will be appreciated in Fig. 2); subsequent outbound packets destined for the remote node that initiated the inner connection must have VPN NAT (source-in NAT as in Fig. 4) applied to the outbound destination IP address before the packet is encapsulated inside the inner IPsec connection, and appropriate to the mode of that connection. This propagation of the VPN NAT rule specific for a given inner IPsec connection is necessary because their may be multiple inner connections from multiple remote nodes, and each must have its own unique IP address on the internal side of the 'first node' (50 in Fig 2). This is not taught by Sirsuresh.

Regarding claim 4, which depends from claim 3, Sirsuresh does not contain an inner IPsec connection. Sirsuresh also does not contain an outer IPsec connection, nor does Sirsuresh encapsulate a packet in the inner connection and then in the outer connection.

Regarding claim 5, which depends from claims 3 and 4,

discussed above, Sirsuresh does not save any address translation rule included within said packet, as claimed. Hence Sirsuresh does not anticipate claim 5.

Regarding claim 6, which depends from claims 3, 4 and 5, discussed above, Sirsuresh does not contain nested IPsec connections, of any depth. Hence Sirsuresh does not contain "iteratively executing said decapsulating step". Hence Sirsuresh does not anticipate claim 6.

Applicants, therefore, request that the rejections of claims 1, 3-6, and 10 under 35 U.S.C. 102 over Sirsuresh be reconsidered and the claims allowed.

35 U.S.C. 103

Claims 2, 7-9, 11-14, and 16-22 have been rejected under 35 U.S.C. 103(a) over Srisuresh.

Claim 15 has been rejected under 35 U.S.C. 103(a) over Srisuresh in view of Hluchyj et al. (U.S. Patent 6,282,193, hereinafter Hluchyj.)

Applicants have canceled claim 2.

With respect to claim 7, as the claim is amended and as the art reference is discussed above, Sirsuresh does not teach nested IPsec connections. And Sirsuresh does not contain nested IPsec connections with coincident endpoints. Hence Sirsuresh does not contain, nor make obvious, anything like "automatically maintaining between said remote client and said gateway nested IP security connections with local coincident endpoints.

With respect to claim 8, which depends from claim 7, Sirsuresh does not contain an inner and an outer IPsec connection. Hence their use with VPN NAT are not taught by the reference.

With respect to claim 9, which depends from claims 7 and 8, Sirsuresh does not teach "responsive to receiving an inbound nested packet from said client on said outer connection..." because Sirsuresh does not have or mention or address the problems associated with nested IPsec connections, as previously discussed with respect to claims 1 and 10. Hence this claim is not taught by Sirsuresh.

With respect to claims 11 & 16, applicants have amended the claim to clarify that both connections are IP security connections. Claim 11 states "Method for extending virtual private network (VPN) network address translation (NAT) to include support for nested connections with coincident endpoints...". As discussed above with respect to claims 1, 3 and 10, Sirsuresh does not deal with nested IPsec connections nor with nested IPsec connection with coincident endpoints. Further, that claims 11 & 16 recite "... without requiring any special configuration for the inner connection...". Sirsuresh does not address how to do this.

As set forth specifically or by implication in various claims, several aspects solved in the current invention that Sirsuresh does not address, nor mention, include automatic initialization of inner IPsec connection VPN NAT rule for an outer IPsec connection, the automatic generation of the implicit VPN NAT rule (implicit MAP), the automatic IP address pool selection for the VPN NAT rule, the automatic loading of the VPN NAT rule on the outer connection, the later automatic propagation of the VPN NAT rule to the newly created inner IPsec connection, the application of the VPN NAT rule to outbound traffic to be doubly encapsulated in the two IPsec connections, and all this support for multiple

levels of nested connections, and for multiple inner connections within a single outer connection. Applicants argue that these solutions are not taught and cannot be implied from the teachings of Sirsuresh.

With respect to claim 12, which depends from claim 11, Sirsuresh does not teach or suggest starting an inner IPsec connection because there is no outer connection.

With respect to claim 13, which depends from claims 11 and 12, Sirsuresh neither teaches nor suggests anything like "saving any VPN NAT rule included within said packet". And then, "applying said NAT rule...".

With respect to claim 14, which depends from claims 11-13, Sirsuresh does not mention, nor contain any suggestion of "iteratively executing said decapsulating step...". Sirsuresh' figures contain no loops, nor does the specification suggestion that looping might be necessary. Sirsuresh text does not contain a single mention of nested IPsec connections, nor of arbitrarily nested IPsec connections, which would be somewhat surprising since the whole focus of Sirsuresh is "...Tunnel-mode IPsec for NAT Domains" (title of the document). Again, note the

'tunnel-mode' as used in the title refers to IPsec tunnel mode (again, see IP Security Basics, below), and not to nesting of IPsec connections (which may be tunnel mode or not).

With respect to claims 17 & 18, which are related as the Examiner observes to the inventions set forth in claims 1 & 10, Applicants assert the same distinctions with respect to Sirsuresh as previously discussed with respect to claims 1 and 10. Applicants do not traverse the Examiner's assertion that it is well known in the art to implement certain computer methods with software - but the rationale given seems a bit strained (that is, because software is very flexible). These claims are presented in support of licensing considerations, and the software aspects per se are not relied upon for distinguishing the art.

With respect to claims 19-22, these claims are structured similarly to claims 3-6, as the Examiner observes. Applicants refer the Examiner to the discussion above with respect to claims 3-6 for distinguishing Sirsuresh. Again, these claims are presented in support of licensing considerations, and the software aspects per se are not relied upon for distinguishing the art

With respect to claim 15, Applicants agree that Hluchyj mentions L2TP, but not in the context of anything like claims 11-13. The point that Sirsuresh did not anticipate nor make obvious the base and intervening claims, has been made. However, to narrow the issues, Applicants cancel claim 15 without prejudice.

For the benefit of the Examiner, Applicants append as an attachment to this Amendment, a tutorial on IP Security (IPSec), drawing upon relevant standards publications.

Applicants urge that the rejection of claims 2, 7-9, 11-14, and 16-22 be reconsidered and withdrawn.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1, 3-14, and 16-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should

differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. BODEN, ET AL.

By

Shelley M Beckstrand
Reg. No. 24,886

Date: 28 Jun 2005

Shelley M Beckstrand, P.C.
Patent Attorney
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545

ATTACHMENT

- -

IP Security basics

With respect to VPN NAT, the important thing to note in the following summary is when the IP header of the packet is included in the IPsec protocol operations. This is indicated by the graphic showing 'scope' under each depiction of packet parts.

This is important because VPN NAT changes the IP addresses in the original IP header (rather than the tunnel IP header, if there is one).

So, for example, for AH in transport mode, note that the scope of AH's authentication is the entire packet, including the original IP header. Only ESP in transport mode does not include the original IP header.

From RFC2402 IP Authentication Header (AH)

AH in transport mode

```
IP packet before:          ip,     tcp, data
IP packet after:           ip, ah, tcp, data

Scope of authentication: |<---------------->|
```

Mutable fields; set to 0 or a predictable value before ICV calculation.
Immutable fields; source IP address, destination IP address, (and others)

AH in tunnel mode

```
IP packet before:                      ip, tcp, data
IP packet after:           newip, ah, ip, tcp, data

Scope of authentication:  |<----------------------->|
```

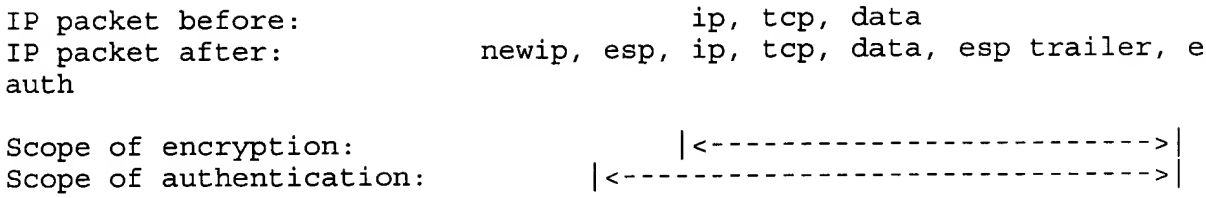
From RFC2406 IP Encapsulating Security Payload (ESP)

ESP in transport mode

```
IP packet before:          ip,      tcp, data
IP packet after:           ip, esp, tcp, data, esp trailer, esp auth

Scope of encryption:                |<---------------------->|
Scope of authentication:       |<--------------------------->|
```

ESP in tunnel mode



From RFC2401 (Security Architecture for the Internet Protocol) & RFC2409 (Internet Key Exchange)

1. SA's are unidirectional; hence 2 SAs needed for each IPsec connection
2. An SA is uniquely identified by {spi, dip, IPsec proto}.
3. If ESP & AH both used the SA needed for each IPsec proto; hence 4 SAs needed for each such IPsec connection
4. SAs are transport or tunnel mode.
5. When AH & ESP are both used, AH header is before the ESP header
6. IKE uses ISAKMP, Oakley to negotiate keys. These negotiations contain IDx, where x = {ii, ir, ui, ur, ci, cr}. The 2nd letter is for 'initiator' or 'responder'. The 1st letter is for phase 1 (i), phase 2 (u) or client (c) negotiations. Basically, these are IP addresses. After decapsulation from any IPsec protocol, the source and destination IP addresses in the resulting IP header must agree with the appropriate IDs negotiated via IKE.